

AMENDMENTS TO THE CLAIMS

1 1.-2. (Canceled)

1 3. (Currently amended) A method ~~as recited in Claim 2 wherein generating the updated~~  
2 ~~key value further comprises:~~ of automatically generating an updated key value for a  
3 segment of keystream for use in a cipher, with forward security, the method comprising  
4 the computer-implemented steps of:  
5 receiving a location value that identifies a location of the segment within the keystream;  
6 generating the updated key value corresponding to the identified segment and based on a  
7 current key value by performing:  
8 creating and storing values in a memory that correspond to a logical tree, wherein the tree  
9 represents the keystream, wherein each leaf node of the tree represents a  
10 particular keystream segment associated with a discrete location in the keystream,  
11 and wherein an order of each leaf node in pre-order traversal of the tree  
12 corresponds to a sequential order of all keystream segments;  
13 creating and storing an ordered plurality of data elements, wherein each of the data  
14 elements is identifiable by a node value that is associated with a unique leaf node  
15 or intermediate node in the tree, and wherein each of the data elements stores a  
16 keystream segment;  
17 advancing to the updated key by outputting that particular keystream segment stored in a  
18 next data element from among the ordered plurality of data elements, and  
19 updating the ordered plurality of data elements to discard used data elements;  
20 seeking a future key without discarding the updated key by locating a highest internal  
21 node in the tree that is an ancestor node of that node corresponding to the updated  
22 key and applying one or more pseudo-random functions to each node in the tree  
23 that is traversed from the highest internal node to a node representing the future  
24 key.

1 4. (Currently amended) A method as recited in Claim 3, wherein ~~generating the updated~~  
2 ~~key value further seeking~~ comprises generating the key value based on the steps of:

3 selecting a highest-ordered element from among the plurality of data elements;  
4 if the selected element is not associated with a leaf node, then:  
5       storing, in a new highest-ordered element among the plurality of data elements, a  
6       first new key value that is determined by applying a first pseudo-random  
7       function to the selected element;  
8       generating a second new key value by applying a second pseudo-random function  
9       to the selected element.

1 5. (Currently amended) A method as recited in Claim 43, wherein ~~generating the updated~~  
2 ~~key value~~ advancing further comprises generating the updated key value based on the  
3 steps of:  
4 returning, as the updated key value, a segment of the keystream associated with the node  
5 identified in the selected next node value when such node is a leaf node;  
6 returning, as the key value that is generated, a segment of the keystream associated with  
7 the second new node value when the node identified in the selected next node  
8 value is not a leaf node.

1 6. (Original) A method as recited in Claim 3, wherein generating the updated key value  
2 further comprises generating the key value based on the steps of:  
3 determining a current location value;  
4 identifying an internal node of the tree having a highest node number that is an ancestor  
5 of a first node corresponding to the received location value and of a second node  
6 corresponding to the current location value;  
7 determining a path from the identified internal node to the first node;  
8 traversing the path while applying a first pseudo-random key updating function to the  
9 then-current key value during each leftward downward transition and applying a  
10 second pseudo-random function during each rightward downward transition.

1 7. (Original) A method as recited in Claim 6, wherein generating the updated key value  
2 further comprises generating the updated key value based on the steps of:

3 storing, in a new highest-ordered element among the plurality of data elements, each new  
 4 key value that is generated as part of applying the first and second pseudo-random  
 5 functions;  
 6 generating, as the updated key value, the new key value that stored in the highest-ordered  
 7 element among the plurality of data elements, when the first node is reached in  
 8 traversing the path.

1 8. (Currently amended) A method as recited in Claim 23, wherein each edge of the tree is  
 2 associated with a distinct pseudo-random function that, when applied to a current key,  
 3 results in generating a new updated key.

1 9. (Currently amended) A method as recited in Claim 23, wherein each edge leading  
 2 leftward and downward from a first node to a second node is associated with a first  
 3 pseudo-random key updating function, and wherein each edge leading rightward and  
 4 downward from the first node to a third node is associated with a second pseudo-random  
 5 key updating function.

1 10. (Currently amended) A method as recited in Claim 69, wherein each of the pseudo-  
 2 random functions receives, as input, a first keystream segment and generates, as output, a  
 3 second keystream segment based on updating the first keystream segment in a pseudo-  
 4 random manner, such that determining the first keystream segment based on the second  
 5 keystream segment is computationally infeasible.

1 11. (Currently amended) A method as recited in Claim 43, further comprising the steps of  
 2 distributing the updated key value to each member of a multicast group for use in secure  
 3 communications among the multicast group.

1 12. (Currently amended) A method of automatically generating an updated key value for a  
 2 segment of keystream for use in a cipher, with forward security, the method comprising  
 3 the computer-implemented steps of:  
 4 receiving a location value that identifies a location of the segment within the keystream;

5 generating the updated key value corresponding to the identified segment and based on a  
6 current key value with forward security ~~and without relying on a key management~~  
7 ~~process for providing such forward secrecy;~~ security, wherein determining  
8 another key value based on the current key, the updated key, and state values that  
9 are stored during the generating is computationally infeasible; by performing:  
10 creating and storing values in a memory that correspond to a logical tree, wherein the tree  
11 represents the keystream, wherein each leaf node of the tree represents a  
12 particular keystream segment associated with a discrete location in the keystream,  
13 and wherein an order of each leaf node in pre-order traversal of the tree  
14 corresponds to a sequential order of all keystream segments;  
15 creating and storing an ordered plurality of data elements, wherein each of the data  
16 elements is identifiable by a node value that is associated with a unique leaf node  
17 or intermediate node in the tree, and wherein each of the data elements stores a  
18 keystream segment;  
19 selecting a highest-ordered element from among the plurality of data elements;  
20 if the selected element is not associated with a leaf node, then:  
21 storing, in a new highest-ordered element among the plurality of data elements, a  
22 first new key value that is determined by applying a first pseudo-random  
23 function to the selected element;  
24 generating a second new key value by applying a second pseudo-random function  
25 to the selected element;  
26 returning, as the updated key value, a segment of the keystream associated with the node  
27 identified in the selected next node value when such node is a leaf node;  
28 returning, as the key value that is generated, a segment of the keystream  
29 associated with the second new node value when the node identified in the  
30 selected next node value is not a leaf node;  
31 determining a current location value;  
32 identifying an internal node of the tree having a highest node number that is an ancestor  
33 of a first node corresponding to the received location value and of a second node  
34 corresponding to the current location value;  
35 determining a path from the identified internal node to the first node;

36 traversing the path while applying a first pseudo-random key updating function to  
37 the then-current key value during each leftward downward transition and  
38 applying a second pseudo-random function during each rightward  
39 downward transition;  
40 storing, in a new highest-ordered element among the plurality of data elements, each new  
41 key value that is generated as part of applying the first and second pseudo-random  
42 functions;  
43 generating, as the updated key value, the new key value that stored in the highest-  
44 ordered element among the plurality of data elements, when the first node  
45 is reached in traversing the path.

1 13.-18. (Canceled)

1 19. (Currently amended) An apparatus for automatically generating an updated key value  
2 for a segment of keystream for use in a cipher, with forward security, comprising:  
3 means for receiving a location value that identifies a location of the segment within the  
4 keystream;  
5 means for generating the updated key value ~~corresponding to the identified segment and~~  
6 ~~based on a current key value with forward security and without relying on a key~~  
7 ~~management process for providing such forward secrecy; and wherein~~  
8 ~~determining another key value based on the current key, the updated key, and~~  
9 ~~state values that are stored during the generating is computationally infeasible,~~  
10 comprising:  
11 means for creating and storing values in a memory that correspond to a logical tree,  
12 wherein the tree represents the keystream, wherein each leaf node of the tree  
13 represents a particular keystream segment associated with a discrete location in  
14 the keystream, and wherein an order of each leaf node in pre-order traversal of the  
15 tree corresponds to a sequential order of all keystream segments;  
16 means for creating and storing an ordered plurality of data elements, wherein each of the  
17 data elements is identifiable by a node value that is associated with a unique leaf

18 node or intermediate node in the tree, and wherein each of the data elements  
19 stores a keystream segment;  
20 means for advancing to the updated key by outputting that particular keystream segment  
21 stored in a next data element from among the ordered plurality of data elements,  
22 and updating the ordered plurality of data elements to discard used data elements;  
23 means for seeking a future key without discarding the updated key by locating a highest  
24 internal node in the tree that is an ancestor node of that node corresponding to the  
25 updated key and applying one or more pseudo-random functions to each node in  
26 the tree that is traversed from the highest internal node to a node representing the  
27 future key.

- 1 20. (Currently amended) An apparatus for automatically generating an updated key value  
2 for a segment of keystream for use in a cipher, with forward security, comprising:  
3 a network interface that is coupled to the data network for receiving one or more packet  
4 flows therefrom;  
5 a processor;  
6 one or more stored sequences of instructions which, when executed by the processor,  
7 cause the processor to carry out the steps of:  
8 receiving a location value that identifies a location of the segment within the  
9 keystream;  
10 generating the updated key value corresponding to the identified segment and  
11 based on a current key value ~~with forward security and without relying on~~  
12 ~~a key management process for providing such forward secrecy; and~~  
13 ~~wherein determining another key value based on the current key, the~~  
14 ~~updated key, and state values that are stored during the generating is~~  
15 ~~computationally infeasible, by performing:~~  
16 creating and storing values in a memory that correspond to a logical tree, wherein the tree  
17 represents the keystream, wherein each leaf node of the tree represents a  
18 particular keystream segment associated with a discrete location in the keystream,  
19 and wherein an order of each leaf node in pre-order traversal of the tree  
20 corresponds to a sequential order of all keystream segments;

21 creating and storing an ordered plurality of data elements, wherein each of the data  
22 elements is identifiable by a node value that is associated with a unique leaf node  
23 or intermediate node in the tree, and wherein each of the data elements stores a  
24 keystream segment;  
25 advancing to the updated key by outputting that particular keystream segment stored in a  
26 next data element from among the ordered plurality of data elements, and  
27 updating the ordered plurality of data elements to discard used data elements;  
28 seeking a future key without discarding the updated key by locating a highest internal  
29 node in the tree that is an ancestor node of that node corresponding to the updated  
30 key and applying one or more pseudo-random functions to each node in the tree  
31 that is traversed from the highest internal node to a node representing the future  
32 key.

1 21.-22. (Canceled)

1 23. (Currently amended) An apparatus as recited in Claim ~~22~~19, wherein the means for  
2 ~~generating the updated key value seeking~~ further comprises means for selecting a highest-  
3 ordered element from among the plurality of data elements; means, if the selected  
4 element is not associated with a leaf node, for storing, in a new highest-ordered element  
5 among the plurality of data elements, a first new key value that is determined by applying  
6 a first pseudo-random function to the selected element, and for generating a second new  
7 key value by applying a second pseudo-random function to the selected element.

1 24. (Currently amended) An apparatus as recited in Claim ~~23~~19, wherein the means for  
2 generating the updated key value further comprises means for returning, as the updated  
3 key value, a segment of the keystream associated with the node identified in the selected  
4 next node value when such node is a leaf node; means for returning, as the key value that  
5 is generated, a segment of the keystream associated with the second new node value  
6 when the node identified in the selected next node value is not a leaf node.

1 25. (Currently amended) An apparatus as recited in Claim ~~22~~19, wherein the means for  
2 generating the updated key value further comprises ~~generating the key value based on the~~  
3 ~~steps of:~~  
4 means for determining a current location value;  
5 means for identifying an internal node of the tree having a highest node number that is an  
6 ancestor of a first node corresponding to the received location value and of a  
7 second node corresponding to the current location value;  
8 means for determining a path from the identified internal node to the first node;  
9 means for traversing the path while applying a first pseudo-random key updating function  
10 to the then-current key value during each leftward downward transition and  
11 applying a second pseudo-random function during each rightward downward  
12 transition.

1 26. (Currently amended) An apparatus as recited in Claim 25, wherein the means for  
2 generating the updated key value further comprises means for storing, in a new highest-  
3 ordered element among the plurality of data elements, each new key value that is  
4 generated as part of applying the first and second pseudo-random functions; means for  
5 generating, as the updated key value, the new key value that stored in the highest-ordered  
6 element among the plurality of data elements, when the first node is reached in traversing  
7 the path.

1 27. (Currently amended) An apparatus as recited in Claim ~~24~~19, wherein each edge of the  
2 tree is associated with a distinct pseudo-random function that, when applied to a current  
3 key, results in generating a new updated key.

1 28. (New) An apparatus as recited in Claim 20, wherein the instructions for seeking further  
2 comprise instructions for performing:  
3 selecting a highest-ordered element from among the plurality of data elements;  
4 if the selected element is not associated with a leaf node, then:



5           storing, in a new highest-ordered element among the plurality of data elements, a  
6           first new key value that is determined by applying a first pseudo-random  
7           function to the selected element;  
8           generating a second new key value by applying a second pseudo-random function  
9           to the selected element.

1   29.   (New) An apparatus as recited in Claim 20, wherein the instructions for advancing  
2           further comprise instructions for performing:  
3           returning, as the updated key value, a segment of the keystream associated with the node  
4           identified in the selected next node value when such node is a leaf node;  
5           returning, as the key value that is generated, a segment of the keystream associated with  
6           the second new node value when the node identified in the selected next node  
7           value is not a leaf node.

1   30.   (New) An apparatus as recited in Claim 20, wherein the instructions for generating the  
2           updated key value further comprise instructions for performing:  
3           determining a current location value;  
4           identifying an internal node of the tree having a highest node number that is an ancestor  
5           of a first node corresponding to the received location value and of a second node  
6           corresponding to the current location value;  
7           determining a path from the identified internal node to the first node;  
8           traversing the path while applying a first pseudo-random key updating function to the  
9           then-current key value during each leftward downward transition and applying a  
10          second pseudo-random function during each rightward downward transition.

1   31.   (New) An apparatus as recited in Claim 20, wherein the instructions for generating the  
2           updated key value further comprise instructions for performing:  
3           storing, in a new highest-ordered element among the plurality of data elements, each new  
4           key value that is generated as part of applying the first and second pseudo-random  
5           functions;

6 generating, as the updated key value, the new key value that stored in the highest-ordered  
7 element among the plurality of data elements, when the first node is reached in  
8 traversing the path.

1 32. (New) An apparatus as recited in Claim 20, wherein each edge of the tree is associated  
2 with a distinct pseudo-random function that, when applied to a current key, results in  
3 generating a new updated key.

1 33. (New) An apparatus as recited in Claim 20, wherein each edge leading leftward and  
2 downward from a first node to a second node is associated with a first pseudo-random  
3 key updating function, and wherein each edge leading rightward and downward from the  
4 first node to a third node is associated with a second pseudo-random key updating  
5 function.

1 34. (New) An apparatus as recited in Claim 33, wherein each of the pseudo-random  
2 functions receives, as input, a first keystream segment and generates, as output, a second  
3 keystream segment based on updating the first keystream segment in a pseudo-random  
4 manner, such that determining the first keystream segment based on the second  
5 keystream segment is computationally infeasible.

1 35. (New) An apparatus as recited in Claim 20, further comprising instructions for  
2 performing distributing the updated key value to each member of a multicast group for  
3 use in secure communications among the multicast group.